

ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction and translation logic. The cryptographic instruction is received by a computing device as part of an instruction flow. The cryptographic instruction prescribes one of the cryptographic operations. The translation logic translates the cryptographic instruction into micro instructions. The micro instructions are ordered to direct the computing device to load a second input text block and to execute the one of the cryptographic operations on the second input text block prior to directing the computing device to store an output text block corresponding to a first input text block. Consequently, the output text block is stored during execution of the one of the cryptographic operations on the second input text block.